Предотвращение утечек данных средствами EDRM и DLP

Андрей Рыбин, *директор по развитию, PERIMETRIX*

Главный источник конкурентоспособности бизнеса сегодня — эффективное использование передовых технологий, создающих дополнительную ценность для клиентов, генерирующих новые потоки доходов. Для компаний, осознавших это, безопасность и конфиденциальность данных значит больше оптимизации затрат, поскольку становится драйвером дохода и роста бизнеса.

Постоянные утечки данных заставляют потребителей с сомнением относиться к бизнесам, пренебрегающим киберугрозами. Пытаясь защитить свои данные, компании приходят к пониманию, что основанный на защите сетевого периметра подход к безопасности **Perimeter-Based Security** (PBS) уже не соответствует современным угрозам.

С позиции PBS утечка происходит в тот момент, когда конфиденциальные данные покидают периметр компании. Поэтому системы предотвращения утечек первоначально фокусировались на контроле над каналами, по которым информация может покинуть корпоративный периметр. Но в цифровой организации подход PBS не способен защитить от нарушителей, действующих внутри доверенной сети, недобросовестных контрагентов, получивших доступ к конфиденциальным данным, противостоять угрозам, связанным с использованием технологий цифровой мобильности (BYOD, коворкинг, работа дома и т.п.).

Отличным от Perimeter-Based Security и наиболее перспективным, на наш взгляд, является информационно-центричный подход к обеспечению безопасности (**Data-Centric Security**, DCS), при котором фокус контроля переносится с содержимого каналов передачи данных на действия, выполняемые с данными. Следование такому подходу позволяет идентифицировать и защитить все ценные информационные активы, строго контролировать доступ к конфиденциальным данным, обеспечить эффективное выполнение бизнес-процессов компании внутри защищенной цифровой экосистемы на протяжении всего жизненного цикла данных. DCS позволяет в полной мере использовать преимущества развитой логики ABAC (Attribute-Based Access Control), формулировать политики безопасности в терминах, понятных бизнес-владельцам данных. Использование DCS требует высокой степени осознанности бизнес-процессов и квалифицированного менеджмента информационной безопасности.

Наиболее популярные сегодня технологии, решающие задачу предотвращения утечек данных двумя различными способами, – это DLP и IRM/EDRM.

DLP-решения традиционно являются одним из компонентов подхода PBS. Блокировка нежелательной передачи данных на основе анализа содержимого каналов, реализуемая DLP, с определенной вероятностью позволяет предотвратить утечку, но может и помешать нормальному выполнению бизнес-процессов. Зачастую основной задачей, возлагаемой на DLP, становится мониторинг с целью проведения расследований. Основные ограничения DLP-систем связаны с невозможностью отслеживания всех возможных каналов утечки и форматов данных, а также с необходимостью соблюдения норм информационного права. Кроме того, при использовании DLP возникают серьезные проблемы при контроле шифрованного трафика, запароленных архивов, файлов, хранящихся в облаках и передаваемых контрагентам.

Самое сложное при внедрении DLP – определение данных, которые необходимо защищать, и выявление всех возможных каналов утечки. Кроме того, приходится ограничивать использование программ, протоколов и типов данных, которые не обрабатываются DLP-решением.

В основе решений класса **EDRM (Enterprise Digital Rights Management)**, позволяющих контролировать действия с данными, находится сочетание нескольких технологических приемов: неотрывная классификация контента, шифрование защищаемых данных, обязательная аутентификация пользователя и гранулярные политики безопасности, определяющие допустимые действия с данными в зависимости от полномочий пользователей.

Благодаря использованию EDRM неавторизованные пользователи не смогут распорядиться защищаемой информацией, при этом все попытки доступа протоколируются. С помощью EDRM можно не только запретить или разрешить доступ пользователя к файлу, но и обеспечить контроль того, как именно пользователи работают с ценными цифровыми объектами – документами, письмами, чертежами, изображениями и т.д.

С учетом сегодняшнего ландшафта угроз информационной безопасности речь не стоит о выборе между DLP и IRM/EDRM, наоборот, требуется их совместное применение в рамках подхода DCS. Интеграция DLP и EDRM – передовой метод борьбы с утечками данных. DLP – по-прежнему хорошее решение для мониторинга коммуникаций, опознавания конфиденциального содержимого с последующим оповещением или блокировкой передачи данных, EDRM – для обеспечения безопасного документооборота, в который вовлечено ограниченное число ответственных сотрудников организации и, возможно, внешних контрагентов.

Если использование DLP в российских компаниях уже стало обычной практикой, то готовность к внедрению EDRM показывают лишь флагманы цифрового бизнеса. В ближайшем будущем нас ждет рост количества инсталляций EDRM-систем и, с учетом импортозамещения, российским производителям этого ПО открываются возможности роста продаж. Потребителям и интеграторам российских EDRM-решений будет интересно наблюдать, как они начнут "обрастать" новым востребованным функционалом, который сейчас присутствует только в западных продуктах.

Компания PERIMETRIX – российский разработчик информационно-центричных систем безопасности.

Perimetrix SafeSpace™ – комплексное программное решение управления электронными данными, позволяющее обеспечить конфиденциальность и целостность электронной информации ограниченного доступа при ее хранении, обработке и передаче. В основе решения – концепция управления жизненным циклом информации ограниченного доступа и уникальная технология контроля перемещений электронной информации. Решение позволяет обеспечить защищенное исполнение пользователем и приложениями рабочего процесса, ограничивая при этом всю другую, не относящуюся к выполнению бизнес-процесса активность пользователей, приложений и процессов. Применение политик "режима" хранения, обработки и передачи классифицированных данных происходит динамически, в момент доступа к классифицированным электронным данным.

Программный комплекс сертифицирован ФСТЭК России (сертификат № 3658 от 15.11.2016 г., действителен до 15.11.2019 г., соответствие РД, ТУ и НДВ4).

Внедрение Perimetrix SafeSpace™ позволяет выполнять требования 149-ФЗ от 27.07.2006 г. "Об информации, информационных технологиях и защите информации" и 98-ФЗ от 29.07.2004 г. "О коммерческой тайне".

Класс продукта – EDRM. Не DLP.

NM
АДРЕСА И ТЕЛЕФОНЫ ООО "ПЕРИМЕТРИКС" см. стр. 52